

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077145

(43)Date of publication of application : 15.03.2002

(51)Int.CI. H04L 9/32
G06F 1/00

(21)Application number : 2000-259706

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 29.08.2000

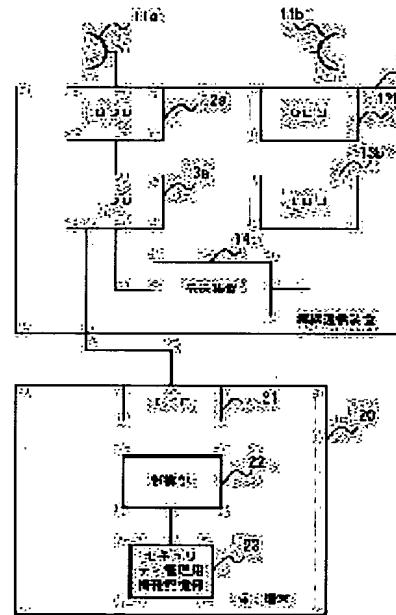
(72)Inventor : HOSAKA MITSURU

(54) SECURITY MANAGING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To realize security of maintenance and supervisory of communication system or the like with simple constitution.

SOLUTION: When a maintenance terminal 20 is connected with radio equipment 10, information for security management of the terminal 20 and that of the radio equipment 10 are compared with each other. When coincidence is obtained, the terminal 20 is so controlled that operation is possible. When coincidence is not obtained, the terminal 20 is so controlled that operation is not possible.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2002-77145

(P2002-77145A)

(43)公開日 平成14年3月15日(2002.3.15)

(51)Int.C1.7

H 0 4 L 9/32

G 0 6 F 1/00 3 7 0

識別記号

F I

G 0 6 F 1/00 3 7 0 E 5J104
H 0 4 L 9/00 6 7 5 A
6 7 3 B

テマコード(参考)

審査請求 未請求 請求項の数5 O L

(全8頁)

(21)出願番号 特願2000-259706(P2000-259706)

(22)出願日 平成12年8月29日(2000.8.29)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 保坂 充

東京都日野市旭が丘3丁目1番地の1 株式
会社東芝日野工場内

(74)代理人 100071054

弁理士 木村 高久

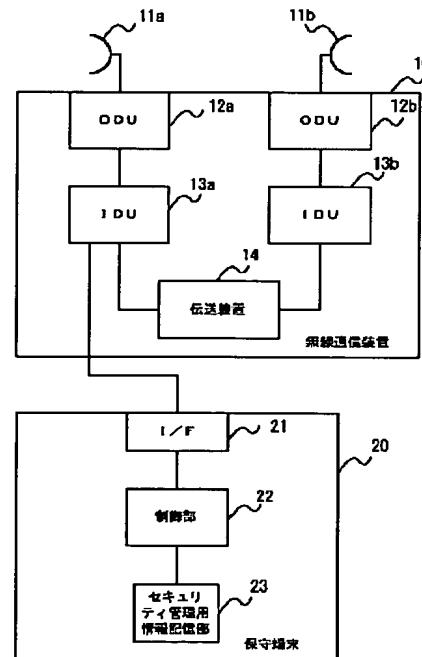
F ターム(参考) 5J104 AA07 KA02 KA04 NA05

(54)【発明の名称】セキュリティ管理方法

(57)【要約】

【課題】 通信システム等の保守、監視のセキュリティを簡単な構成により実現する。

【解決手段】 無線装置10に保守端末20が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば、この保守端末20の動作を可能にし、不一致であれば、この保守端末20を動作不可に制御する。



無線通信装置と保守端末の構成図

【特許請求の範囲】

【請求項 1】 据付型の第1の装置に対して可搬型の第2の装置を接続して前記第1の装置のデータ設定を行うシステムにおけるセキュリティ管理方法において、前記第1の装置および前記第2の装置にそれぞれにセキュリティ管理用情報を記憶し、前記第1の装置に対する前記第2の装置の接続に際して、前記第1の装置および前記第2の装置間で前記セキュリティ管理用情報の照合を行い、該照合結果に基づき前記第1の装置に対する前記第2の装置によるデータ設定を許可することを特徴とするセキュリティ管理方法。

【請求項 2】 前記第1の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶された前記第2の装置を接続した場合は、前記第2の装置のセキュリティ管理用情報を用いて前記第1の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする請求項1記載のセキュリティ管理方法。

【請求項 3】 前記第1の装置に前記セキュリティ管理用情報が記憶されていない前記第2の装置を接続した場合は、前記第1の装置のセキュリティ管理用情報を用いて前記第2の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする請求項1記載のセキュリティ管理方法。

【請求項 4】 前記第1の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶されていない前記第2の装置を接続した場合は、前記第1の装置および前記第2の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする請求項1記載のセキュリティ管理方法。

【請求項 5】 前記第1の装置は、通信システムを構成する複数の通信装置の内の1つの通信装置であり、

前記第2の装置は、前記通信システムの保守、管理を行う保守端末であることを特徴とする請求項1記載のセキュリティ管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信システム等の保守、管理のセキュリティを実現するセキュリティ管理方法に関する。

【0002】

【従来の技術】従来、据付型の複数の無線通信装置から構成される通信システムの全体の監視、制御は、上記複数の無線通信装置のいずれかに接続された監視制御装置

(NMS)により行われている。

【0003】また、上記通信システムの複数の無線通信装置を個別に設定、保守する場合は、制御対象となる無線通信装置に可搬型の保守端末を接続することにより行われている。

【0004】例えば、上記通信システムの複数の無線通信装置うちの特定の無線通信装置の警報状態を調べる場合、若しくは、上記無線通信装置の装置名称等を設定する場合、若しくは、上記無線通信装置の使用周波数を設定する場合、若しくは、上記無線通信装置の警報出力論理を設定する場合、若しくは、上記無線通信装置のログイン名またはパスワード等を個別に設定する場合は、当該無線通信装置に上記可搬型の保守端末を接続して、この保守端末を用いてこの通信システムの各種情報の監視若しくは設定を行う。

【0005】

【発明が解決しようとする課題】ところで、上記保守端末は、特定の通信システムに対応して設計、開発されており、例えば、この保守端末を誤って他の通信システムの無線通信装置に接続した場合、若しくは故意に他の通信システムの無線通信装置に接続した場合は、この他の通信システムの無線通信装置の情報を誤って変更してしまったり、他の通信システムの無線通信装置の情報を不当に収集してしまったりするという事態が発生した。

【0006】例えば、ある通信システムにおける無線通信装置の増設時に、この通信システムとは異なる通信システムのために開発された保守端末をこの増設した無線通信装置に接続して、各種設定を行った場合は、この増設した無線通信装置にこの通信システムに許可されていない周波数を設定してしまうことがあります、この場合は、通信システム間で混信が発生するという問題があり、また、不当に他の通信システムの情報を収集してしまうという問題が発生し、これにより通信システム間のセキュリティが保てないという問題が発生した。

【0007】そこで、この発明は、通信システム等の保守、監視のセキュリティを簡単な構成により実現することを可能にしたセキュリティ管理方法を提供することを目的とする。

【0008】

【課題を解決するための手段】この発明のセキュリティ管理方法は、据付型の第1の装置に対して可搬型の第2の装置を接続して前記第1の装置のデータ設定を行うシステムにおけるセキュリティ管理方法において、前記第1の装置および前記第2の装置にそれぞれにセキュリティ管理用情報を記憶し、前記第1の装置に対する前記第2の装置の接続に際して、前記第1の装置および前記第2の装置間で前記セキュリティ管理用情報の照合を行い、該照合結果に基づき前記第1の装置に対する前記第2の装置によるデータ設定を許可することを特徴とする。

【0009】すなわち、この発明のセキュリティ管理方法によれば、第1の装置に第2の装置が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば第1の装置および第2の装置が1つのシステムとして動作し、不一致であれば、第1の装置および第2の装置は1つのシステムとしては動作しない。

【0010】このような構成によると、2つの装置を接続した時点でそれぞれの装置が当該システムのために設置した装置であるかどうかが判別可能になり、例えば、他のシステムでの使用のための装置を持ち込んでシステムに組み込む不正使用を防止することができ、システムのセキュリティを確保することができる。

【0011】また、この発明のセキュリティ管理方法は、前記第1の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶された前記第2の装置を接続した場合は、前記第2の装置のセキュリティ管理用情報を用いて前記第1の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする。

【0012】また、この発明のセキュリティ管理方法は、前記第1の装置に前記セキュリティ管理用情報が記憶されていない前記第2の装置を接続した場合は、前記第1の装置のセキュリティ管理用情報を用いて前記第2の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする。

【0013】また、この発明のセキュリティ管理方法は、前記第1の装置に前記セキュリティ管理用情報が記憶されていない状態において、前記セキュリティ管理用情報が記憶されていない前記第2の装置を接続した場合は、前記第1の装置および前記第2の装置に前記セキュリティ管理用情報を自動的に記憶することで、前記第1の装置に対する前記第2の装置によるデータ設定を可能にしたことを特徴とする。

【0014】すなわち、第1の装置と第2の装置のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を使って未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設定する。

【0015】このような構成によると、装置故障や装置の増設対応などにより、新しく装置をシステムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【0016】

【発明の実施の形態】以下、この発明に係わるセキュリティ管理方法の実施の形態を添付図面を参照して詳細に説明する。

【0017】図1は、この発明に係わるセキュリティ管理方法を適用する通信システムの一例を示すシステム構成図である。

【0018】この通信システムは、複数台、図1においては4台の無線通信装置10-1～10-4を無線回線でリング状に接続して構成される。

【0019】また、4台の無線通信装置10-1～10-4の内の無線通信装置10-3には、この通信システムの全体の監視、制御を行う監視制御装置(NMS)100が接続されている。

【0020】また、図1においては、この通信システムを構成する無線通信装置10-1～10-4のうちの無線通信装置10-4を個別に調整若しくは保守のために、この無線通信装置10-4に保守端末20を接続した場合を示している。

【0021】なお、図1においては、保守端末20を無線通信装置10-4に接続した場合を示しているが、この保守端末20は、他の無線通信装置10-1～10-3にも同様に接続することができる。

【0022】図2は、図1に示した無線通信装置10-1～10-4および保守端末20の構成を示すブロック図である。

【0023】なお、図2において、無線通信装置10は、図1に示した無線通信装置10-1～10-4の内の1台の無線通信装置を示している。

【0024】図2において、この無線通信装置10は、アンテナ11a, 11b、アンテナ11a, 11bにそれぞれ接続され、主に屋外に設置されるODU(アウトドアユニット)12a, 12b、ODU12a, 12bにそれぞれ接続され、主に屋内に設置されて主に無線通信のベースバンド信号の処理およびODU12a, 12bの制御を行うIDU(インドアユニット)13a, 13b、IDU13a, 13bに接続される伝送装置14を具備して構成される。

【0025】ここで、伝送装置14は、例えば、ATM伝送装置を用いて構成されており、予め設定された通信バスに基づきIDU13a, 13b間の伝送情報をスルーリしたり、この伝送装置14に接続された図示しない端末に出力したりする動作を行う。ここで、ATMの場合の通信バスの設定とはVOI/VCI毎に伝送情報をどのポートに出力するかの設定を行う。なお、この伝送装置14としては、ATM伝送装置に限らず、例えば、SDH方式等の同期多重方式を用いた伝送装置を採用することもできる。

【0026】なお、図2の構成において、保守端末20は、IDU13a若しくは13bに接続されるが、図2においては、保守端末20をIDU13aに接続した場合を示している。

【0027】すなわち、図2において、IDU13a, 13bは、図3に示しように構成されている。

【0028】図3は、図2に示したIDU13a、13bをIDU13として示すもので、ODU12a若しくは12bに接続されるとともに、伝送装置14に接続される送信部131および受信部部132、この送信部131および受信部部132を制御するとともに、このIDU13の全体動作を制御する制御部133、この発明に係わるセキュリティ管理情報を記憶するセキュリティ管理情報部134、図2に示した保守端末20との通信のインターフェースをなす保守端末用インターフェース（保守端末用I/F）135を具備して構成される。

【0029】さて、図2において、保守端末20は、無線通信装置10（IDU13a）との通信のインターフェースをなすインターフェース部（I/F）21、この保守端末20の全体動作を統括制御する制御部22、この発明に係わるセキュリティ管理用情報を記憶するセキュリティ管理用情報記憶部23を具備して構成される。

【0030】ここで、保守端末20は、図1に示した通信システムの各無線通信装置10-1～10-4の各種情報を個別に設定、保守するもので、この通信システムのために専用に開発されたものである。

【0031】この保守端末20の設定監視動作としては、

- 1) 無線通信装置の警報状態
- 2) 無線通信装置の装置名称等の設定
- 3) 無線通信装置の使用周波数の設定
- 4) 無線通信装置の警報出力論理
- 5) 無線通信装置のログイン名またはパスワード等の設定

等を行う。

【0032】なお、この実施の形態においては、無線通信装置10のIDU13aのセキュリティ管理用情報記憶部134に記憶されているセキュリティ管理用情報と保守端末20のセキュリティ管理用情報記憶部23に記憶されているセキュリティ管理用情報とは同一の情報が使用されているが、保守端末20がこの無線通信装置10により構築される通信システムのために開発されたものであることが識別できれば、IDU13aのセキュリティ管理用情報記憶部134に記憶されているセキュリティ管理用情報と保守端末20のセキュリティ管理用情報記憶部23に記憶されているセキュリティ管理用情報とは同一でなくてもよい。

【0033】また、無線通信装置10のセキュリティ管理用情報記憶部134に記憶されているセキュリティ管理用情報および保守端末20のセキュリティ管理用情報記憶部23に記憶されているセキュリティ管理用情報は、セキュリティの程度に応じて任意の情報量、任意の形態の情報を使用することができる。

【0034】また、無線通信装置の使用周波数、すなわち、この場合、ODU12aの無線周波数の設定は、IDU13aを介して設定される。

【0035】図4は、図2に示した保守端末20の動作を説明するフローチャートである。

【0036】図4において、この保守端末20は、まず、無線通信装置10に接続されたかを調べる（ステップ301）。ここで、無線通信装置10に接続されていないと判断されると、ステップ301に戻り、無線通信装置10に接続されるのを待つ。

【0037】ステップ301で、無線通信装置10に接続されたと判断されると（ステップ301でYES）、

10 無線通信装置10のセキュリティ管理用情報記憶部134からセキュリティ管理用情報を取り出し（ステップ302）、無線通信装置10のセキュリティ管理用情報記憶部134にはセキュリティ管理用情報が設定済かを調べる（ステップ303）。

【0038】ここで、無線通信装置10のセキュリティ管理用情報記憶部134にセキュリティ管理用情報が設定済であると判断されると（ステップ303でYES）、次に、保守端末20のセキュリティ管理用情報記憶部23からセキュリティ管理用情報を取り出す（ステップ304）。

【0039】そして、保守端末20のセキュリティ管理用情報記憶部23にはセキュリティ管理用情報が設定済かを調べる（ステップ305）。ここで、保守端末20のセキュリティ管理用情報記憶部23にセキュリティ管理用情報が設定済であると判断されると（ステップ305でYES）、無線通信装置10のセキュリティ管理用情報記憶部134から取り出したセキュリティ管理用情報と保守端末20のセキュリティ管理用情報記憶部23から取り出したセキュリティ管理用情報を比較する（ステップ306）。

【0040】この比較において、無線通信装置10のセキュリティ管理用情報記憶部134から取り出したセキュリティ管理用情報と保守端末20のセキュリティ管理用情報記憶部23から取り出したセキュリティ管理用情報とが一致すると（ステップ306で一致）、この保守端末20は、この通信システムに組み込み可能であると判断して、この保守端末20の使用中状態となる（ステップ307）。

【0041】そして、次に、無線通信装置10との接続が断かを調べ（ステップ308）、接続断でないと判断されると（ステップ308でNO）、ステップ307に戻り、この保守端末20の使用中状態を続ける。

【0042】また、ステップ308で、無線通信装置10との接続が断であると判断されると（ステップ308でYES）、この保守端末20の使用中状態を終了してステップ301へ戻る。

【0043】また、ステップ306で、無線通信装置10のセキュリティ管理用情報記憶部134から取り出したセキュリティ管理用情報と保守端末20のセキュリティ管理用情報記憶部23から取り出したセキュリティ管

理用情報とが一致しないと判断されると（ステップ306で不一致）、この保守端末20は、この通信システムに組み込み不可であると判断して、この保守端末20の使用不可状態となる（ステップ309）。

【0044】そして、次に、無線通信装置10との接続が断かを調べ（ステップ310）、接続断でないと判断されると（ステップ310でNO）、ステップ309に戻り、この保守端末20の使用不可状態を続けるが、ステップ310で、無線通信装置10との接続が断であると判断されると（ステップ310でYES）、ステップ301へ戻る。

【0045】また、ステップ303で、無線通信装置10のセキュリティ管理用情報記憶部134にセキュリティ管理用情報が設定されていないと判断されると（ステップ303でNO）、次に、保守端末20のセキュリティ管理用情報記憶部23からセキュリティ管理用情報を取り出し（ステップ311）、保守端末20のセキュリティ管理用情報記憶部23にはセキュリティ管理用情報が設定済かを調べる（ステップ312）。

【0046】ここで、保守端末20のセキュリティ管理用情報記憶部23にセキュリティ管理用情報が設定済であると判断されると（ステップ312でYES）、未設定の無線通信装置10のセキュリティ管理用情報記憶部134に保守端末20のセキュリティ管理用情報記憶部23に設定されているセキュリティ管理用情報を設定し（ステップ313）、保守端末20の使用中状態となる（ステップ307）。

【0047】すなわち、保守端末20のセキュリティ管理用情報記憶部23にはセキュリティ管理用情報が設定されているが、無線通信装置10のセキュリティ管理用情報記憶部134にはセキュリティ管理用情報が設定されていない場合は、設定済みの保守端末20のセキュリティ管理用情報記憶部23に記憶されたセキュリティ管理用情報を用いて未設定の無線通信装置10のセキュリティ管理用情報記憶部134にセキュリティ管理用情報を自動設定して、保守端末20の使用を可能にする。

【0048】また、ステップ312で、保守端末20のセキュリティ管理用情報記憶部23にセキュリティ管理用情報が設定されていないと判断されると（ステップ312でNO）、この場合は、無線通信装置10のセキュリティ管理用情報記憶部134および保守端末20のセキュリティ管理用情報記憶部23に新たなセキュリティ管理用情報を自動設定して保守端末20の使用中状態となる（ステップ307）。

【0049】すなわち、無線通信装置10のセキュリティ管理用情報記憶部134および保守端末20のセキュリティ管理用情報記憶部23にそれぞれセキュリティ管理用情報が設定されていない場合は、無線通信装置10のセキュリティ管理用情報記憶部134および保守端末20のセキュリティ管理用情報記憶部23にそれぞれ新

たなセキュリティ管理用情報を自動設定して、保守端末20の使用を可能にする。

【0050】また、ステップ305で、保守端末20のセキュリティ管理用情報記憶部23にセキュリティ管理用情報が設定されていないと判断されると（ステップ305でNO）、未設定の保守端末20のセキュリティ管理用情報記憶部23に無線通信装置10のセキュリティ管理用情報記憶部134に設定されているセキュリティ管理用情報を設定し、保守端末20の使用中状態となる（ステップ307）。

【0051】すなわち、無線通信装置10のセキュリティ管理用情報記憶部134にはセキュリティ管理用情報が設定されているが、保守端末20のセキュリティ管理用情報記憶部23にはセキュリティ管理用情報が設定されていない場合は、設定済みの無線通信装置10のセキュリティ管理用情報記憶部134に記憶されたセキュリティ管理用情報を用いて未設定の保守端末20のセキュリティ管理用情報記憶部23にセキュリティ管理用情報を自動設定して、保守端末20の使用を可能にする。

【0052】このような構成によると、無線通信装置10に保守端末20を接続した時点で保守端末20が当該通信システムのための装置であるかどうかが判別可能になり、例えば、他の通信システムでの使用のための装置を持ち込んでこの通信システムに組み込む不正使用を防止することができ、通信システムのセキュリティを確保することができる。

【0053】また、無線通信装置10と保守端末20のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を用いて未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設定するように構成したので、装置故障や装置の増設対応などにより、新しく装置をこの通信システムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【0054】図5は、図2に示した無線通信装置10に保守端末20を接続した場合に、保守端末20と無線通信装置10との間で行われる信号シーケンスの一例を示す図である。

【0055】図5において、保守端末20が無線通信装置10に接続されると、保守端末20から無線通信装置10へデータ表示要求が送信される。

【0056】このデータ表示要求を受信した無線通信装置10は、保守端末20へこのデータ表示要求に対するデータ表示応答を返信する。

【0057】これにより、保守端末20では、無線通信装置10からの表示情報を表示することが可能になる。

【0058】図6は、図2に示した無線通信装置10に保守端末20を接続した場合に、保守端末20と無線通

信装置10との間で行われる信号シーケンスの他の例を示す図である。

【0059】図6においては、図5に示した、保守端末20から無線通信装置10へのデータ表示要求の送信および無線通信装置10から保守端末20へのデータ表示応答の返信に加えて、保守端末20から無線通信装置10へのデータ設定要求の送信および無線通信装置10から保守端末20へのデータ設定応答の返信が可能になるように構成されている。

【0060】このような構成によると、保守端末20では、無線通信装置10からの表示情報の表示だけではなく、無線通信装置10に対するデータ設定が可能になる。

【0061】なお、上述した実施の形態においては、この発明を通信システムに適用した場合を示したが、この発明に係わるセキュリティ管理方法は、上述したような通信システムに限らず、セキュリティ管理の必要な他のシステムにも同様に適用することができる。

【0062】また、この発明は上述した実施の形態の構成に限定されず、その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることは言うまでもない。

【0063】

【発明の効果】以上説明したようにこの発明によれば、第1の装置に第2の装置が接続された時点で互いのセキュリティ管理用情報を比較し、一致していれば1つのシステムとして動作し、不一致であれば、1つのシステムとしては動作しないように構成したので、2つの装置を接続した時点でそれぞれの装置が当該システムのために設置した装置であるかどうかが判別可能になり、例えば、他のシステムでの使用のための装置を持ち込んでシステムに組み込む不正使用を防止することができ、システムのセキュリティを確保することができる。

【0064】また、第1の装置と第2の装置のセキュリティ管理用情報を比較したときに一方のセキュリティ管理用情報が未設定である場合は、設定済みのセキュリティ管理用情報を使って未設定のセキュリティ管理用情報を若しくは両者のセキュリティ管理用情報を自動的に設

定するように構成したので、装置故障や装置の増設対応などにより、新しく装置をシステムに組み込む場合には、自動的にセキュリティ管理用情報の設定が行われるので、システム構築を迅速に行うことができる。

【図面の簡単な説明】

【図1】この発明に係わるセキュリティ管理方法を適用する通信システムの一例を示すシステム構成図である。

【図2】図1に示した無線通信装置および保守端末の構成を示すブロック図である。

【図3】図2に示したIDUの詳細構成を示すブロック図である。

【図4】図2に示した保守端末20の動作を説明するフローチャートである。

【図5】図2に示した無線通信装置10に保守端末20を接続した場合に、保守端末20と無線通信装置10との間で行われる信号シーケンスの一例を示す図である。

【図6】図2に示した無線通信装置10に保守端末20を接続した場合に、保守端末20と無線通信装置10との間で行われる信号シーケンスの他の例を示す図である。

【符号の説明】

10、10-1～10-4 無線通信装置

11a, 11b アンテナ

12a, 12b ODU (アウトドアユニット)

13, 13a, 13b IDU (インドアユニット)

14 伝送装置

20 保守端末

21 インタフェース (I/F)

22 制御部

30 23 セキュリティ管理用情報記憶部

100 監視制御部 (NMS)

131 送信部

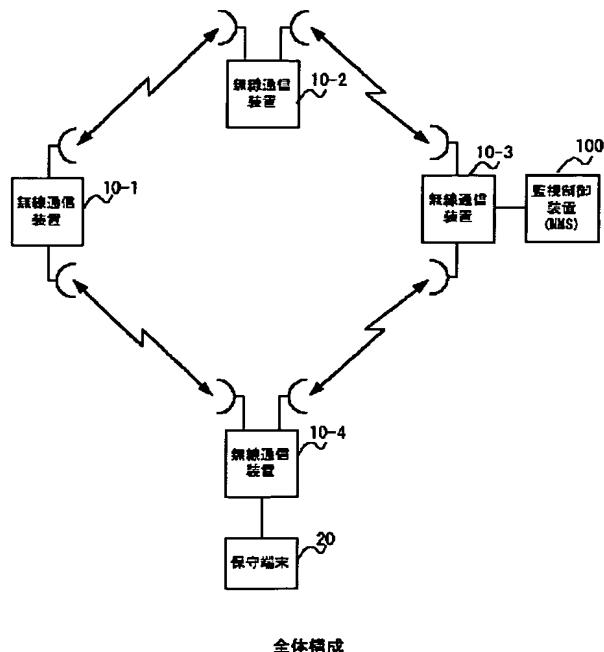
132 受信部

133 制御部

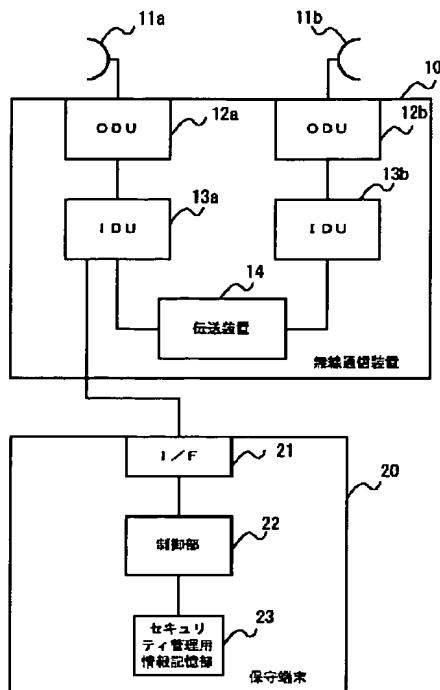
134 セキュリティ管理用情報記憶部

135 保守端末用インターフェース (保守端末用 I/F)

【図1】

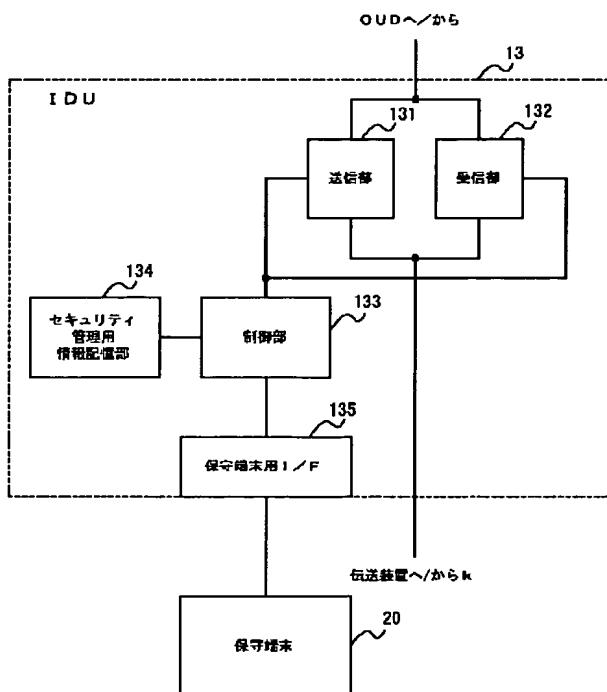


【図2】

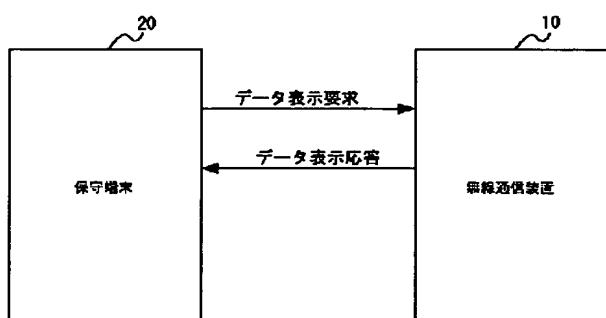


無線通信装置と保守端末の構成図

【図3】



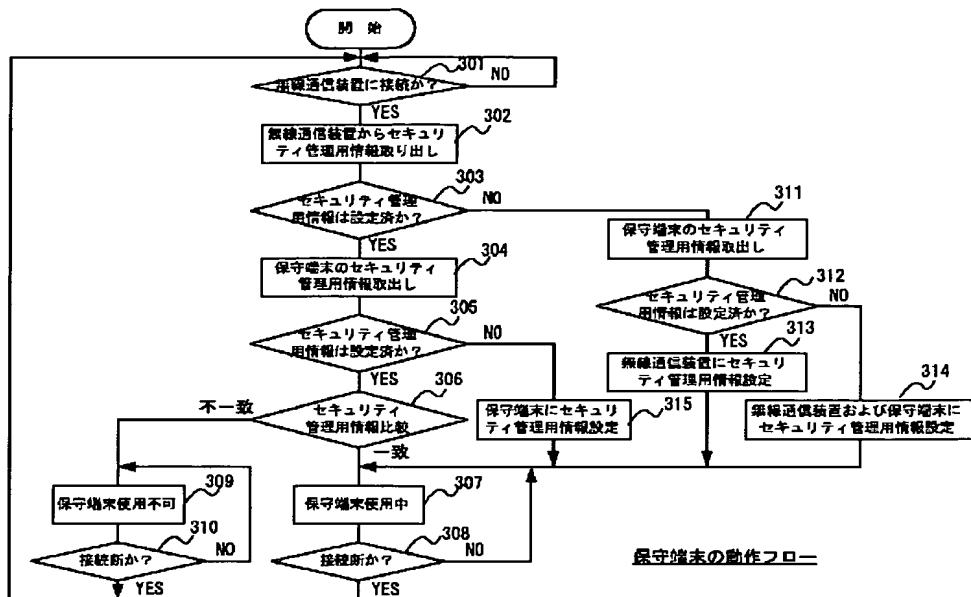
【図5】



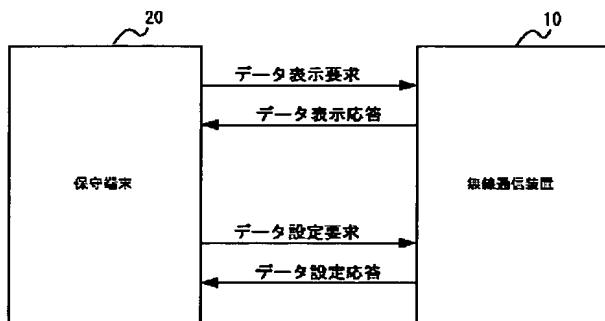
保守端末と無線通信装置との間の信号シーケンス図

IDUの構成図

【図4】



【図6】



保守端末と無線通信装置との間の往復の信号シーケンス図